Miles N. Clark, Esq.
Nevada Bar No. 13848
LAW OFFICES OF MILES N. CLARK, LLC
5510 S. Fort Apache Rd, Suite 30
Las Vegas, Nv 89148
Phone: (702) 856-7430
Fax: (702) 552-2370
Email: miles@milesclarklaw.com

Samuel J. Strauss, Esq.*
Raina C. Borrelli, Esq.*
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Phone: (872) 263-1100
Fax: (872) 263-1109
sam@straussborrelli.com
raina@straussborrelli.com
* *Pro hac vice forthcoming*

Attorneys for Plaintiff and Proposed Class

IN THE UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

MICHAEL J. MONTOYA, on behalf of himself and all others similarly situated, Plaintiff(s), v. RIVERSIDE RESORT AND CASINO, LLC, Defendant.	Case No.: 2:24-cv-01692 **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff, Michael J. Montoya ("Plaintiff"), on behalf of himself and all others similarly situated, states as follows for his class action complaint against Defendant Riverside Resort and Casino LLC ("Riverside" or "Defendant"):

INTRODUCTION

1. On or around July 25, 2024, Riverside became aware that it had lost control over its computer network and the highly sensitive personal information stored on the computer network in a data breach by cybercriminals ("Data Breach"). On information and belief, the Data Breach has impacted current and former customers of Riverside.

2. Riverside is a Nevada-based casino resort that was opened in. Riverside is now home to over 1,300 slot and video poker machines and 35 live gaming tables and has undergone numerous expansions throughout the last 20 years. Riverside's workforce is comprised of over 2,000 employees.[1]

3. Due to Defendant's intentionally obfuscating language, it is unclear when the Data Breach precisely occurred and how long cybercriminals had unfettered access to Plaintiff's and the Class's highly sensitive information. However, on information and belief, the breach took place prior to July 25, 2024.

4. Following an internal investigation, Defendant learned cybercriminals gained unauthorized access to current and former customers' personally identifiable information ("PII"), including but not limited to their name and Social Security number.

5. On or about September 5, 2024–six weeks after the Data Breach was discovered–Defendant finally began notifying Plaintiff and Class Members about the Data Breach ("Breach Notice"). A copy of Plaintiff's Breach Notice is attached as Exhibit A and a sample of a Breach Notice is attached as Exhibit B.

6. Upon information and belief, cybercriminals were able to breach Defendant's

[1] Laughlin: The Man & The Town, Riverside Resort and Casino LLC, https://www.riversideresort.com/don-laughlin-history-founder-riverside-resort-casino/ (last visited September 11, 2024).

systems because Defendant failed to adequately train its employees on cybersecurity, failed to adequately monitor its agents, contractors, vendors, and suppliers in handling and securing the PII of Plaintiff, and failed to maintain reasonable security safeguards or protocols to protect the Class's PII—rendering them easy targets for cybercriminals.

7. Defendant's Breach Notice obfuscated the nature of the breach and the threat it posed—refusing to tell its current and former customers how many people were impacted, how the breach happened, when the Breach happened, or why it took the Defendant six weeks to begin notifying victims that cybercriminal had gained access to their highly private information.

8. Defendant's failure to timely report the Data Breach made the victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

9. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

10. In failing to adequately protect current and former customers' information, adequately notify them about the breach, and obfuscating the nature of the breach, Defendant violated state law and harmed a staggering number of customers.

11. Plaintiff and the Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

12. Plaintiff is a customer of Defendant and is a Data Breach victim.

13. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before

the Data Breach, the private information of Plaintiff and the Class was exactly that—private. Not anymore. Now, their private information is permanently exposed and unsecure.

PARTIES

14. Plaintiff, Michael J. Montoya, is a natural person and citizen of Arizona, residing in Williams, Arizona, where he intends to remain.

15. Defendant Riverside Resort and Casino, Inc. is a Domestic Corporation with its principal place of business at 1650 S. Casino Dr., Laughlin, NV, 89029.

JURISDICTION & VENUE

16. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. There are over 100 putative Class Members.

17. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in Nevada, and regularly conducts business in Nevada.

18. Venue is proper in this Court under because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Riverside Resort & Casino

19. Riverside is a "premier gaming destination and year-round playground."[2] Located in Laughlin, Nevada, "[n]early 5 million annual visitors retreat to this desert oasis renowned for a seemingly endless list of activities."[3]

20. As part of its business, Defendant receives, collects, and maintains the highly

[2] *Id.*
[3] *Id.*

sensitive PII of its current and former customers. In doing so, Defendant implicitly promises to safeguard their PII.

21. After collecting its customers' PII, Defendant maintains the PII in its computer systems. On information and belief, Defendant maintains former customers' PII for years after their relationship is terminated.

22. In collecting and maintaining customers' PII, Defendant agreed it would safeguard the data in accordance with its internal policies as well as state law and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.

23. Indeed, Defendant understood the importance of adequate cybersecurity measures, declaring in its Privacy Policy any personal information collected is "stored on secure servers" that "are protected by firewalls and a multitude of other industry standard security measures… instituted to ensure the protection of these secure servers from unauthorized access."[4]

24. The Privacy Policy also promises:

a. Riverside has "controls in place that are designed to detect potential data breaches, contain and minimize the loss of data, and conduct forensic investigations of a breach;"

b. Riverside's "staff is required to take reasonable measures to ensure that unauthorized persons cannot view or access your Personal Information;" and

c. Riverside "will take reasonable steps, which are standard in the industry to ensure that the communication methods used to support the Riverside Resort and Casino do not permit connection or communication by methods that have

[4] Privacy Policy, Riverside Resort and Casino LLC, https://www.riversideresort.com/privacy-policy/ (last visited September 11, 2024).

known security weaknesses or vulnerabilities."[5]

25. Defendant understood the need to protect its customers' PII and prioritize its data security.

26. Despite recognizing its duty to do so, on information and belief, Defendant has not implemented reasonably cybersecurity safeguards or policies to protect customers' PII or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to customers' PII.

The Data Breach

27. Plaintiff is a customer of Riverside.

28. As a condition of receiving services from Riverside, customers were required to disclose their PII to Defendant, including but not limited to, their names and Social Security numbers. Defendant used that PII to facilitate the provision of services to Plaintiff and required Plaintiff to provide that PII to obtain services.

29. On information and belief, Riverside collects and maintains former and current customers' unencrypted PII in its computer systems.

30. In collecting and maintaining the PII, Riverside implicitly agrees it will safeguard the data using reasonable means according to its internal policies and federal law.

31. According to the Breach Notice, Defendant claims that on July 25, 2024 it "learned of suspicious activity in its environment." Ex. A. Due to Defendant's obfuscating information, the precise dates on which the Data breach occurred and how long cybercriminals had access to Plaintiff's and the Class's most sensitive information is unclear.

[5] *Id.*

32. Defendant's investigation determined that "an unauthorized third party potentially accessed and acquired certain files." Ex. A. Upon completion of its investigation, Defendant revealed that the files involved in the breach included customers' names and Social Security numbers. Ex. A.

33. In other words, the Data Breach investigation revealed Riverside's cyber and data security systems were completely inadequate and allowed cybercriminals to access files containing a treasure trove of its customers' highly private information.

34. Additionally, Defendant admitted that PII was actually stolen during the Data Breach, confessing that the information was not just accessed, but was "acquired" from Riverside's system. Ex. A.

35. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class's PII for theft and sale on the dark web.

36. On or about September 5, 2024–about a month after Defendant completed its investigation– Defendant finally began notifying Plaintiff and Class Members about the Data Breach.

37. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

38. And when Defendant did notify Plaintiff and the Class of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, encouraging Plaintiff and the Class to:

a. "remain vigilant against incidents of identity theft and fraud;"

b. "review your account statements;"

c. "monitor your credit reports for suspicious or unauthorized activity;"

d. "contact your financial institution and all major credit bureaus to inform them of such a breach;" and

e. "take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file." Ex. B.

39. Despite its duties and alleged commitments to safeguard PII, Defendant did not in fact follow industry standard practices in securing customers' PII, as evidenced by the Data Breach.

40. On information and belief, Defendant has several months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers.

41. Even with several months of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

42. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

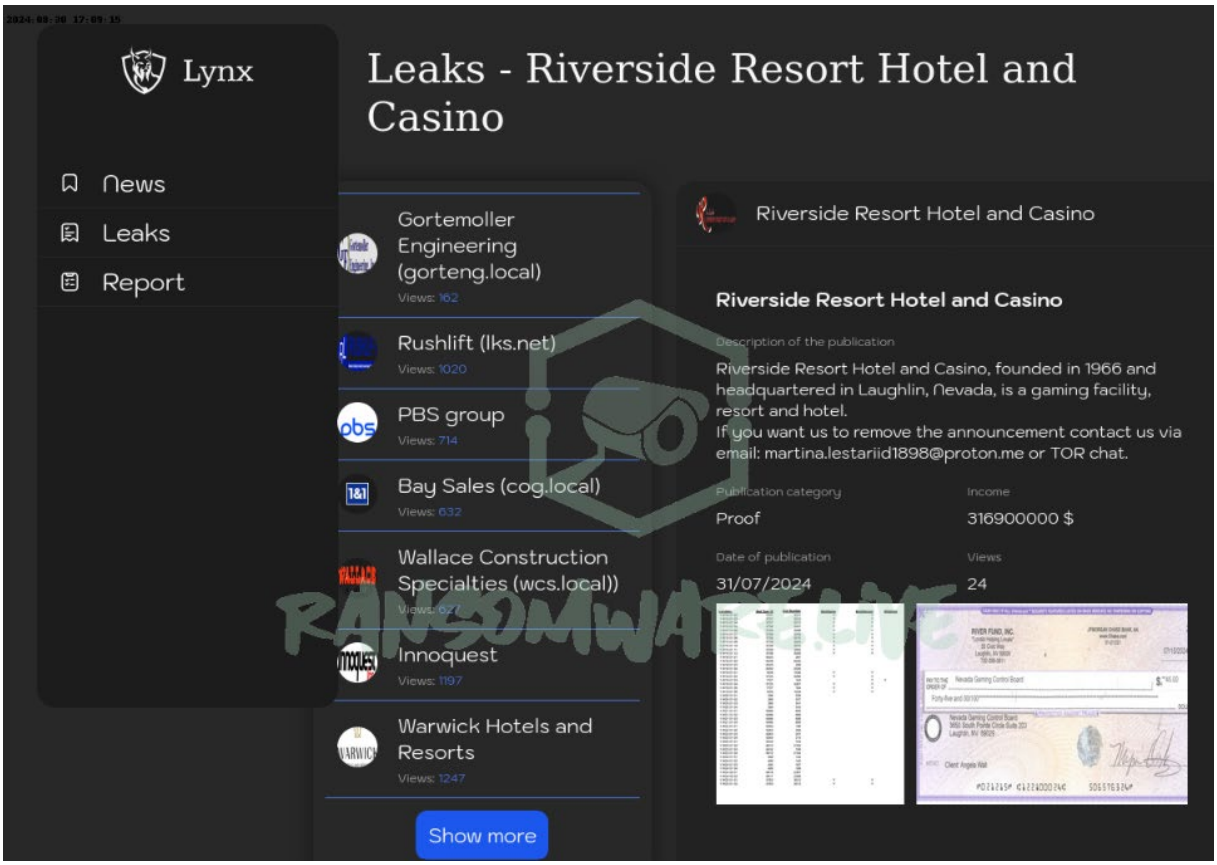
43. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its customers' PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from

accessing the PII.

44. Worryingly, the cybercriminals that obtained Plaintiff's and Class members' PII appear to be the notorious ransomware group "Lynx Ransomware"[6]—a ransomware group that emerged in August 2023 that uses double extortion on its victims and is known for "encrypting files and stealing data, demanding ransom payments."[7]

45. Lynx Ransom claimed responsibility for the attack, posting sample screenshots on its dark web portal of information it acquired from Riverside and stating "If you want us to remove the announcement contact us via email… or TOR chat."[8]

[6] @FalconFeeds.io, Twitter (X) (August 30, 2024, 1:03 PM), https://x.com/FalconFeedsio/status/1829580755283923032.
[7] *Id.*
[8] Ransomware.Live, https://images.ransomware.live/screenshots/posts/1119d54e69e7d2a56e0cab879a192a3e.png (last visited September 11, 2024).



46. And as the Harvard Business Review notes, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[9]

47. Thus, on information and belief, Plaintiff's and the Class's stolen PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

The Data Breach was a Foreseeable Risk of Which Defendant was on Notice

48. It is well known that PII, including Social Security numbers, is an invaluable commodity and a frequent target of hackers.

[9] Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back.

49. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[10]

50. In light of recent high profile data breaches, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Riverside knew or should have known that its electronic records would be targeted by cybercriminals.

51. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

52. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

53. In the years immediately preceding the Data Breach, Defendant knew or should have known that its computer systems were a target for cybersecurity attacks, including ransomware attacks involving data theft, because warnings were readily available and accessible via the internet.

54. In November 2023, the Federal Bureau of Investigation issued a Private Industry Notification that, among other things, warned of a trend of "ransomware actors exploiting

[10] Data breaches break record in 2021, CNET (Jan. 24, 2022), https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last visited September 11, 2024).

vulnerabilities in vendor-controlled remote access to casino servers."[11]

55. This warning followed a series of high-profile ransomware attacks on casino and hotel giants in September 2023.[12]

56. According to Katell Thielemen, VP analyst at Gartner, casinos "are an opportunistic target because they have money and the public outcry is less pronounced when they are attacked."[13] Plus, "[t]he gaming industry is heavily regulated and therefore is full of technologies to monitor the movement of clients, croupiers, service workers and funds alike. Every one of these systems is a possible entry point."[14]

57. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[15]

58. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to

---

[11] Private Industry Notification, FBI, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.aha.org/system/files/media/file/2023/11/bi-tlp-clear-pin-ransomware-actors-continue-to-gain-access-through-third-parties-and-legitimate-system-tools-11-7-23.pdf (last visited September 11, 2024).

[12] Ransomware targeting casinos is on the rise, FBI warns, CybersecurityDive, https://www.cybersecuritydive.com/news/ransomware-targets-casinos-fbi/699313/ (last visited September 11, 2024).

[13] *Id.*

[14] *Id.*

[15] Ransomware Mentioned in 1,000+ SEC Filings Over the Past Year, ZDNET (April 30, 2020), https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last visited August 30, 2024).

release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[16]

59. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) ransomware actors were targeting entities such as Defendant, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities such as Defendant, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included threatening to release stolen data.

60. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted PII of thousands of its customers in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII.

61. Before the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack. Notably, data breaches are prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Defendant.

62. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted its customers' Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

Plaintiff's Experience and Injuries

63. Plaintiff Michael Montoya is a customer of Riverside.

64. As a condition of receiving services, Riverside required Plaintiff to provide his PII,

[16] Stop Ransomware Guide, CISA, https://www.cisa.gov/stopransomware/ransomware-guide (last visited August 30, 2024).

including but not limited to his full name and Social Security number.

65. Plaintiff provided his PII to Riverside and trusted that the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

66. Defendant deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about it until six weeks after the Data Breach was discovered.

67. Plaintiff suffered actual injury from the exposure of his PII—which violates his rights to privacy.

68. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

69. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's PII for theft by cybercriminals and sale on the dark web.

70. Defendant also deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about it in a timely manner.

71. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

72. Plaintiff has and will spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Plaintiff fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach.

73. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

74. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

75. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

76. Indeed, following the Data Breach, Plaintiff began experiencing a substantial increase in spam and scam emails, suggesting that his PII has been placed in the hands of cybercriminals.

77. On information and belief, Plaintiff's email was compromised as a result of the Data Breach, as cybercriminals are able to use an individual's PII that is accessible on the dark web, as Plaintiff's is here, to gather and steal even more information.[17]

78. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

79. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

[17] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited August 30, 2024).

80. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiff and the Class have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

81. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

82. The value of Plaintiff's and the proposed Class's PII on the black market is

considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

83. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover, Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

84. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

85. One such example of criminals using PII for profit is the development of "Fullz" packages.

86. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

87. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and the Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and

members of the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

88. Defendant disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII. Defendant's failure to properly notify Plaintiff and the Class of the Data Breach exacerbated Plaintiff's and the Class's injuries by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

89. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

90. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand its network's vulnerabilities; and

e. implement policies to correct security problems.

91. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

92. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

93. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer, data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet its data security obligations.

94. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

95. Several best practices have been identified that—at a minimum—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

96. Other industry standard best practices include: installing appropriate malware

detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

97. Upon information and belief, Frontier failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04).

98. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

99. Plaintiff sues on behalf of himself and the proposed nationwide class ("Class"), defined as follows, pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3):

> All individuals residing in the United States whose PII was compromised in the Data Breach discovered by Riverside in July 2024, including all those individuals who received notice of the breach.

100. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any of Defendant's officers or directors, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

101. Plaintiff reserves the right to amend the class definition.

102. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. The members of the Class are so numerous that joinder of all members of the Class is impracticable. Plaintiff is informed and believes that the proposed Class includes thousands of current and former customers who have been damaged by Defendant's conduct as alleged herein.

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. His interests do not conflict with the Class's interests, and he has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant was negligent in maintaining, protecting, and securing PII;

iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's PII;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

103. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

Count I
Negligence
(On Behalf of Plaintiff and the Class)

104. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

105. Defendant owed to Plaintiff and the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

106. Defendant owed a duty of care to Plaintiff and members of the Class because it was

foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of the Class's PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

107. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

108. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and the Class's personal information and PII.

109. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

110. PII is highly valuable, and Defendant knew, or should have known, the risk in

obtaining, using, handling, emailing, and storing the PII of Plaintiff and members of the Class and the importance of exercising reasonable care in handling it.

111. Defendant breached its duties by failing to exercise reasonable care in handling and securing the personal information and PII of Plaintiff and members of the Class which actually and proximately caused the Data Breach and Plaintiff's and members of the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

112. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

113. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff and Class members' Private Information.

114. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such

as Defendant, of failing to use reasonable measures to protect the Private Information entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the Class members' sensitive Private Information.

115. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

Count II
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

116. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

117. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of receiving services from Defendant. Plaintiff and Class Members provided their PII to Defendant in exchange for Defendant's services.

118. Plaintiff and Class Members reasonably understood that a portion of their payments to Defendant would be by Defendant used to pay for adequate cybersecurity and protection of their PII.

119. Plaintiff and the Class Members accepted Defendant's offers by disclosing their PII to Defendant in exchange for services.

120. Plaintiff and Class Members entered into implied contracts with Defendant under

which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members if and when their data had been breached and compromised. Each such contractual relationship imposed on Defendant an implied covenant of good faith and fair dealing by which Defendant was required to perform its obligations and manage Plaintiff's and Class Members' data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendant.

121. In providing their PII, Plaintiff and Class Members entered into an implied contract with Defendant whereby Defendant, in receiving such data, became obligated to reasonably safeguard Plaintiff's and the other Class Members' PII.

122. In delivering their PII to Defendant, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard that data.

123. Plaintiff and the Class Members would not have entrusted their PII to Defendant in the absence of such an implied contract.

124. Defendant accepted possession of Plaintiff's and Class Members' PII.

125. Had Defendant disclosed to Plaintiff and Class Members that Defendant did not have adequate computer systems and security practices to secure customers' PII, Plaintiff and members of the Class would not have provided their PII to Defendant.

126. Defendant recognized that customers' PII is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and Class Members.

127. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

128. Defendant breached the implied contract with Plaintiff and Class Members by

failing to take reasonable measures to safeguard their data.

129. Defendant breached the implied contract with Plaintiff and Class Members by failing to promptly notify them of the access to and exfiltration of their PII.

130. As a direct and proximate result of the breach of the contractual duties, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Class Members' PII; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their PII; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendant promised when Plaintiff and the proposed class entrusted Defendant with their PII; and (h) the continued and substantial risk to Plaintiff's and Class Members' PII, which remains in the Defendant's possession with inadequate measures to protect Plaintiff's and Class Members' PII.

Count III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

131. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

132. This claim is pleaded in the alternative to the breach of implied contract claim.

133. Upon information and belief, Riverside funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and Class Members.

134. As such, a portion of the payments made by or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Riverside.

135. Plaintiffs and Class Members conferred a monetary benefit on Riverside. Specifically, they purchased goods and services from Defendant and in so doing provided Defendant with their PII. In exchange, Plaintiffs and Class Members should have received from Riverside the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

136. Riverside knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Riverside profited from these transactions and used the PII of Plaintiffs and Class Members for business purposes.

137. In particular, Riverside enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Riverside instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

138. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

139. Defendant acquired the monetary benefit and PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

140. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

141. Plaintiff and Class Members have no adequate remedy at law.

142. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity how their PII is used; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

143. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm.

144. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

//

Count IV
Violation of the Nevada Consumer Fraud Act
Nev. Rev. Stat. § 41.600
(On Behalf of Plaintiff and the Class)

145. Plaintiffs restate and reallege all proceeding factual allegations above as if fully set forth herein.

146. The Nevada Consumer Fraud Act, Nev. Rev. Stat. § 41.600 states in relevant part:

147. An action may be brough by any person who is a victim of consumer fraud.

148. As used in this section, "consumer fraud" means: . . . A deceptive trade practice defined in NRS 598.0915 to 598.0225, inclusive. Nev. Rev. Stat. § 41.600(1) & (2)(e).

149. In turn, Nev. Rev. Stat. § 598.0923(2) provides that "[a] person engages in a 'deceptive trade practice' when in the course of his or her business or occupation he or she knowingly . . . [f]ails to disclose a material fact in connection with the sale or lease of goods or services." *Id.* Riverside violated this provision because it failed to disclose the material fact that its data security measures were inadequate to reasonably safeguard its customers' PII. This is true because, among other things, Riverside was aware of the risks of cyberattacks such as the Data Breach. Riverside knew or should have known that that its data security measures were insufficient to guard against attacks such as the Data Breach. Riverside had knowledge of the facts that constituted the omission. Riverside could have and should have made a proper disclosure prior to providing services to customers by any other means reasonably calculated to inform customers of its inadequate data security measures.

150. Further, Nev. Rev. Stat. § 598.0923(3) provides that "[a] person engages in a 'deceptive trade practice' when in the course of his or her business or occupation he or she knowingly . . . [v]iolates a state or federal statute or regulation relating to the sale or lease of goods or services." *Id.* Riverside violated this provision for several reasons, each of which serves

as an independent basis for violating Nev. Rev. Stat. § 598.0923(3).

151. First, Riverside breached its duty under Nev. Rev. Stat. § 603A.210, which requires any data collector "that maintains records which contain personal information" of Nevada residents to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, . . . use, modification or disclosure." *Id.* Riverside is a "data collector" as defined by Nev. Rev. Stat. § 603A.030. Riverside failed to implement such reasonable security measures, as shown by a system-wide breach of its computer systems during which a threat actor exfiltrated customer PII. Riverside's violation of this statute was done knowingly for the purposes of Nev. Rev. Stat. § 598.0923(3) because Riverside knew or should have known that it would be a target of cyberattacks such as the Data Breach. Riverside knew or should have known that its data security measures were inadequate to protect against cyberattacks such as the Data Breach.

152. Second, Riverside violated Section 5 of the FTC Act, as alleged above. Riverside knew or should have known that its data security measures were inadequate, violated Section 5 of the FTC Act and failed to adhere to the FTC's data security guidance. This is true because Riverside was well aware that the casino industry is a frequent target of cyberattacks such as the Data Breach and the FTC has recommended various data security measures that companies such as Defendant could have implemented to mitigate the risk of a Data Breach. Riverside chose not to follow such guidance and knew or should have known that its data security measures were inadequate to guard against cyberattacks such as the Data Breach. Riverside had knowledge of the facts that constituted the violation. Riverside's violation of Section 5 of the FTC Act serves as a separate actional basis for purposes of violating Nev. Rev. Stat. § 598.0923(3).

153. Riverside engaged in an unfair practice by engaging in conduct that is contrary to

public policy, unscrupulous, and caused injury to Plaintiff and Class Members.

154. Plaintiff and members of the Class were denied a benefit conferred on them by the Nevada legislature.

155. As a direct and proximate result of the foregoing, Plaintiff and Class Members have suffered injuries including, but not limited to actual damages, and in being denied a benefit conferred on them by the Nevada legislature.

156. As a result of these violations, Plaintiffs and Class Members are entitled to an award of actual damages, equitable injunctive relief requiring Defendant to implement adequate data security measures, as well as an award of reasonable attorney's fees and costs. Nev. Rev. Stat. § 41.600(3).

Count V
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

157. Plaintiff restates and realleges all preceding allegations set forth above as if fully alleged herein.

158. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et. seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Consolidated Amended Class Action Complaint.

159. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and whether Riverside is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of

his PII and remains at imminent risk that further compromises of their PII will occur in the future.

160. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that, among other things:

a. Riverside owed a legal duty to secure customers' PII under the common law, Section 5 of the FTC Act, and state data security laws; and

b. Riverside breached and continues to breach this legal duty by failing to employ reasonable measures to secure customers' PII.

161. This Court also should issue corresponding prospective injunctive relief requiring Riverside to employ adequate security protocols consistent with law and industry standards to protect members' PII.

162. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Riverside. The risk of another such breach is real, immediate, and substantial. If another breach at Riverside occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

163. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to Riverside if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Riverside of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Riverside has a pre-existing legal obligation to employ such measures.

164. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach

at Riverside, thus eliminating the additional injuries that would result to Plaintiff, Class Members, and consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff hereby demands that this matter be tried before a jury.

Dated: September 11, 2024

Respectfully Submitted,

/s/ Miles N. Clark
Miles N. Clark, Esq.
Nevada Bar No. 13848
LAW OFFICES OF MILES N. CLARK, LLC
5510 S. Fort Apache Rd, Suite 30
Las Vegas, NV 89148
Phone: (702) 856-7430
Fax: (702) 552-2370
Email: miles@milesclarklaw.com

Samuel J. Strauss*
Raina C. Borrelli*
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
sam@straussborrelli.com
raina@straussborrelli.com
* *Pro hac vice forthcoming*

Attorneys for Plaintiff and Proposed Class